Lurie Besikof Lapidus
& Company, LLP

MAXIMUS – California Healthy Families

Service Auditor's Report on Controls Placed in Operation and Tests of Operating Effectiveness

March 1, 2009 through February 28, 2010

Prepared Pursuant to Statement on Auditing Standards Number 70, As Amended

Table of Contents

Section Page

SECTION ONE

Independent Service Auditor’s Report

SECTION ONE – INDEPENDENT SERVICE AUDITOR'S REPORT

Mr. Bruce Caswell, President, MAXIMUS Operations Group:

We have examined the accompanying description of controls related to MAXIMUS in connection with your contract 02MHF026 with the State of California Managed Risk Medical Insurance Board (MRMIB) related to the California Healthy Families program and the Access for Infants and Mothers (AIM) program (the Project). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the Project's controls that may be relevant to the MRMIB's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and the MRMIB applied the controls contemplated in the design of the Project's controls; and (3) such controls had been placed in operation as of February 28, 2010. The control objectives were specified by Project management. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

The accompanying description does not include, where contractually required control objectives to provide reasonable assurance that for each AIM participant, a birth outcome is ultimately capitated. We believe this control objective should be specified in the Project's description of controls because it would be relevant to the MRMIB.

In our opinion, except for the matter referred to in the preceding paragraph, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of the Project's controls that had been placed in operation as of February 28, 2010. Also, in our opinion, except for the deficiency referred to in the preceding paragraph, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and the MRMIB applied the controls contemplated in the design of the Project's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section Three of this report, to obtain evidence about their effectiveness in meeting the control objectives, described in Section Three of this report, during the period from March 1, 2009 to February 28, 2010. The specific controls and the nature, timing, extent, and results of the tests are listed in Section Three of this report. This information has been provided to the MRMIB and to the auditors of the State of California to be taken into consideration, along with information about the internal control at the MRMIB, when making assessments of control risk for the MRMIB. In our opinion, the controls that were tested, as described in Section Three of this report, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section Three of this report were achieved during the period from March 1, 2009 to February 28, 2010.

The relative effectiveness and significance of specific controls at the Project and their effect on assessments of control risk at the MRMIB are dependent on their interaction with the controls and other factors present at the MRMIB. We have performed no procedures to evaluate the effectiveness of controls at the MRMIB.

The description of controls at the Project is as of February 28, 2010, and information about tests of the operating effectiveness of specific controls covers the period from March 1, 2009 to February 28, 2010. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the Project is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls may alter the validity of such conclusions.

This report is intended solely for use by the management of the Project, MAXIMUS, the MRMIB, the
State of California and the auditors of the State of California.

Lurie Besikof Lapidus & Company, LLP
Lurie Besikof Lapidus & Company, LLP
June 17, 2010

SECTION TWO

Description of Controls Provided by MAXIMUS

SECTION TWO – DESCRIPTION OF CONTROLS PROVIDED BY MAXIMUS

MAXIMUS, Administrative Contractor for the California Healthy Families Program

The administration and computer functions for the State of California Managed Risk Medical Insurance Board (MRMIB) for the MAXIMUS California Healthy Families program and the Access for Infants and Mothers program (the Project) are located in California.

The California Healthy Families program is the California implementation of the Federal State Children's Health Insurance Program (SCHIP), Title XXI Act. The Access for Infants and Mothers program is low-cost health coverage for pregnant women and their newborns implemented by Title 10 of the California Code of Regulations, Chapter 5.6. The MRMIB contracted with MAXIMUS to act as the Administrative Contractor for the two Programs, collectively referred to as the Project. The Project, as the Administrative Contractor, is required to perform the administrative functions including the maintenance of case records, invoicing for health care premiums, collection of premiums, and the maintenance of financial records for the Programs under the direction of the MRMIB.

The Project's administrative functions under the contract with the MRMIB for the programs include data systems supporting fully integrated eligibility, enrollment and financial/accounting systems.

Risk Assessment

The Project has placed into operation a risk assessment process to identify and manage risks that could affect the Project's ability to provide reliable transaction processing for the MRMIB. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks.

Monitoring

The Project's management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities.

Information and Communications

Information Systems

Multiple servers and databases support numerous Project functions from application processing to financial posting.

Control Objectives and Related Description of Control Activities

Information Systems General Controls

Control Objective 1: Controls provide reasonable assurance that the Project Management demonstrates, through attitude, awareness and actions, an atmosphere that enhances the effectiveness of specific policies and procedures. These include controls to provide reasonable assurance that:

- the Project's structure provides appropriate division of responsibilities;
- service levels are defined and managed in a manner that satisfies the case management system requirements and provides a common understanding of performance levels with which the quality of services are measured; and
- third-party services are secure, accurate and available, supporting processing integrity and are defined appropriately in performance contracts.

Description of Control Activities:

Project Oversight Strategy

1.1 Management has mechanisms to obtain feedback from relevant external stakeholders, business process owners, and end-users regarding the quality and usefulness of information technology and information systems.

1.2 The Project monitors its progress against planned performance measures and reacts accordingly to meet established objectives.

Organization and Relationships

1.3 Directors, managers and technicians have adequate knowledge and experience to fulfill their responsibilities.

1.4 Key systems and data have been inventoried and their owners identified.

1.5 Roles and responsibilities of the Project are defined, documented and understood.

1.6 Personnel have sufficient authority to exercise the role and responsibility assigned to them.

1.7 Personnel understand and accept their responsibility regarding internal control.

1.8 Management has implemented a division of roles and responsibilities (segregation of duties) that reasonably prevent a single individual from subverting a critical process.

1.9 Staff evaluations are performed regularly. Employees receive their first written performance evaluation after 90 days of employment.

1.10 All staff including contracted staff and other contract personnel are subject to policies and procedures created to control their activities by the IT function, and to assure the protection of the Project's information assets.

1.11 Significant IT events or failures, e.g., security breaches, major system failures or regulatory failures, are reported to senior management.

Management of Human Resources

1.12 Controls are in place to support appropriate and timely responses to job changes and job terminations so that internal controls and security are not impaired by such occurrences.

Educate and Train Users

1.13 The Project subscribes to a philosophy of continuous learning, providing necessary training and skill development to its employees.

1.14 Established procedures exist for identifying and documenting the training needs of all personnel that use information services in support of the Project.

1.15 Management provides education and ongoing training programs that include ethical conduct, system security practices, confidentiality standards, integrity standards and security responsibilities for all staff.

Assessment of Risks

1.16 The Project has an activity-level risk assessment framework, which is used periodically to assess information risk for achieving business objectives, and it considers the probability and likelihood of threats.

Manage Facilities

1.21 Facilities are adequately secured and managed.

1.22 Data center facilities are equipped with adequate environmental controls to maintain systems and data, including fire suppression, uninterrupted power service (UPS), generator, and appropriate air conditioning.

Compliance with External Requirements

1.23 Control activities are in place and followed to ensure compliance with external requirements, such as regulatory and legal rules.

1.24 Internal events are considered in a timely manner to support continuous compliance with legal and regulatory requirements.

Management of Quality

1.25 Documentation is created and maintained for all significant processes, controls and activities.

1.26 A plan exists to maintain the overall quality assurance of activities, based on the Project plans.

1.27 Documentation standards are in place and have been communicated to all staff, and are supported with training.

1.28 A quality plan exists for significant IT functions (e.g., large system development and deployment projects) and it provides a consistent approach to address both general and project-specific quality assurance activities.

1.29 The quality plan prescribes the type(s) of quality assurance activities (such as reviews, audits, inspections) to be performed to achieve the objectives of the quality plan.

1.30 The quality assurance process includes a review of adherence to policies, procedures and standards.

Manage Performance and Capacity

1.31 IT management monitors the performance and capacity levels of the systems and network.

1.32 IT management has a process in place to respond to suboptimal performance and capacity measures.

1.33 Performance and capacity planning is included in system design and implementation activities.

Monitoring

1.34 Performance indicators or benchmarks, from both internal and external sources, have been defined, and data is collected and reported regarding achievement of these benchmarks.

1.35 Management has established appropriate metrics to effectively manage the day-to-day activities.

1.36 Management monitors delivery of services to identify shortfalls and responds with actionable plans to improve.

Adequacy of Internal Control

1.37 Management monitors the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons and benchmarks.

1.38 Serious deviations in the operation of internal control, including major security, availability and processing integrity events, are reported to senior management.

1.39 Internal control assessments are performed periodically, using self-assessments, to examine whether or not internal controls are operating satisfactorily.

Internal Audit

1.40 Internal Audit engagements are performed based on approval by the audit committee.

Third-Party Services

1.41 A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.

1.42 The selection of vendors for outsourced services is performed in accordance with the Project's vendor management policy.

1.43 Before selection, management determines that potential third parties are properly qualified through an assessment of their capability to deliver the required service.

1.44 Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.

1.45 Procedures exist and are followed to ensure that a formal contract is defined and agreed for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the Project's policies and procedures.

1.46 A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.

Computer Operations Controls

General Operations

Control Objective 2: Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved, or investigated for proper resolution.

Control Objective 3: Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.

Control Objective 4: Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated.

Security and Access Controls

Control Objective 5: Controls provide reasonable assurance that Project information technology (IT) operating systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage, or loss of data.

Control Objective 6: Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.

Acquisition, Development and Change

Control Objective 7: Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms to support case management operating applications.

Control Objective 8: Controls provide reasonable assurance that application software is acquired or developed to effectively support both the California Healthy Families program and the Access for Infants and Mothers program case management operating requirements.

Control Objective 9: Controls provide reasonable assurance that systems are appropriately tested and validated prior to being placed into production processes, and that associated controls operate as intended and support case management operating requirements.

Control Objective 10: Controls provide reasonable assurance that policies and procedures defining required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.

Control Objective 11: Controls provide reasonable assurance that system changes of operational significance are appropriately tested and authorized before movement into production.

Application Processing Controls – Case Management Systems

Input Controls

Control Objective 12: Input controls provide reasonable assurance.

Processing Controls

Control Objective 13: Processing controls provide reasonable assurance.

Output Controls

Control Objective 14: Output controls provide reasonable assurance.

Systems Application Processing Controls – Financial Management Systems

Input Controls

Control Objective 15: Input controls provide reasonable assurance that:

- Originating HFP and AIM source data are entered by trained and authorized persons, and that data preparation procedures are established and followed to minimize errors and omissions, and to allow the input of only valid data into the system.
- Automation is used where possible to reduce errors, increase efficiency and route priority work.
- Authorized source documentation and data is complete and accurate, properly accounted for, and transmitted in a timely manner.
- Error handling procedures detect errors and irregularities and report them for corrective action.
- Source documents are retained and available for reconstruction and legal compliance.

Processing Controls

Control Objective 16: Processing controls provide reasonable assurance that:

- Data is posted to the correct files, completely and accurately.
- Unauthorized changes to data are prevented.
- Database files remain unchanged until authorized processing occurs.
- Procedures assure that balancing of data is made with relevant control totals. Transaction processing can be traced effectively to reconcile disrupted data.
- There is continuity and integrity of stored data.
- Procedures establish development standards, as appropriate, for electronic transaction integrity and authenticity (atomicity, consistency, isolation, and durability).

Output Controls

Control Objective 17: Output controls provide reasonable assurance that:

- Procedures define handling and retention of output. When negotiable instruments are produced, special care should be taken to prevent misuse.
- Procedures define and assure appropriate distribution of IT output.
- Procedures are communicated for physical and logical access to output. Confidentiality of output is defined and taken into consideration in the procedures.
- Procedures assure that both provider and user review output for accuracy and that procedures control errors contained in the output.
- Physical access to output printers and subsequent storage areas is restricted to authorized personnel.

User Control Considerations

The processing of transactions and the Project's control policies and procedures covers only a portion of the overall internal control structure of MRMIB. It is not feasible for the control objectives to be solely achieved by HFP and AIM. Therefore, MRMIB's internal control structure must be evaluated in conjunction with HFP and AIM's control policies and procedures summarized in the report.

SECTION THREE

Information Provided by the Service Auditor

SECTION THREE – INFORMATION PROVIDED BY THE SERVICE AUDITOR

Purpose and Objectives of the Report

This report is intended to provide interested parties with information about the MAXIMUS controls in connection with its contract 02MHF026 with the California Managed Risk Medical Insurance Board (MRMIB) related to the California Healthy Families program and the Access for Infants and Mothers program (the Project), and to provide information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the internal controls at the MRMIB, is intended to assist the MRMIB's auditors in planning the audit of the MRMIB's financial statements and in assessing control risk for assertions in the MRIMIB's financial statements that may be affected by controls at the Project.

Our examination was restricted to the description of controls, control objectives and the related control procedures specified in Section Two by MAXIMUS management and was not extended to procedures described elsewhere in this report but not listed, or to procedures that may be in effect at the user organization. The examination was conducted in accordance with the Statement on Auditing Standards (SAS) No. 70, "Report on the Processing of Transactions by Service Organizations," as amended by SAS Nos. 78, 88, and 98, of the American Institute of Certified Public Accountants. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user organization. If certain complementary controls are not in place at the user organization, MAXIMUS controls may not compensate for such weaknesses.

The description of controls and control objectives are the responsibility of MAXIMUS management. Our responsibility is to express an opinion about whether—

1) The description of controls presents fairly, in all material respects, the relevant aspects of MAXIMUS controls that had been placed in operation as of February 28, 2010.
2) The controls, as described by MAXIMUS, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and if user organizations applied the internal controls contemplated in the design of MAXIMUS controls.
3) The controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by MAXIMUS management, were achieved during the period March 1, 2009 to February 28, 2010.

Tests of Operating Effectiveness

Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions throughout the period of March 1, 2009 to February 28, 2010, for each of the controls listed in Section Three, which are designed to achieve the specific control objectives. In selecting particular tests of the operational effectiveness of controls, we considered: (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

Tests performed of the operational effectiveness of controls are described in general below and in more detail on the following pages:

Type of Test	General Description of Test
Inquiry, or corroborative inquiry	Inquired of appropriate personnel to ascertain the compliance with controls.
Observation	Observed application of specific controls.
Obtained and inspected	Obtained and inspected documents and reports indicating performance of the controls.
Verified	Compared information obtained from two independent sources to verify the operation of the control.
Tested	Reperformed application of the controls.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Information Systems General Controls		
Control Objective 1: Controls provide reasonable assurance that the Project Management demonstrates, through attitude, awareness and actions, an atmosphere that enhances the effectiveness of specific policies and procedures. These include controls to provide reasonable assurance that: • the Project's structure provides appropriate division of responsibilities; • service levels are defined and managed in a manner that satisfies the case management system requirements and provides a common understanding of performance levels with which the quality of services are measured; and • third-party services are secure, accurate and available, supporting processing integrity and are defined appropriately in performance contracts.		
Project Oversight Strategy		
1.1 Management has mechanisms to obtain feedback from relevant external stakeholders, business process owners, and end-users regarding the quality and usefulness of information technology and information systems.	• *Obtained* and *inspected* documentation for the existence of feedback mechanisms from relevant stakeholders, business process owners, and end-users regarding information technology and information systems. The documentation inspected included the following: ▪ Bi-Weekly MRMIB Progress Meeting minutes, ▪ Weekly Tactical Meeting Minutes, ▪ Internal Policy Work Group (IPWG) minutes, and ▪ DHCS and the MRMIB Bi-Weekly Coordination Meeting Minutes.	No relevant exceptions noted
	• *Inquired* of selected Program personnel regarding management's different mechanisms for obtaining and utilizing feedback.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.2 The Project's Management monitors its progress against planned performance measures and reacts accordingly to meet established objectives.	• *Obtained* and inspected documentation for the use of performance measures and the communication of those measures to staff. The documentation inspected includes the following: ▪ Weekly Tactical Meeting minutes, and ▪ California Healthy Families Program (CAHFP).	No relevant exceptions noted
	• *Inquired* of management personnel regarding the weekly staff meetings containing the agenda item reviewing the key metrics.	No relevant exceptions noted.
	• *Tested* a sample of CAHFP Performance Indicators spreadsheets by tracing certain information back to the source documents verifying that the source data agreed to the measurement presented in the spreadsheet.	No relevant exceptions noted.
Organization and Relationships		
1.3 Directors, managers and technicians have adequate knowledge and experience to fulfill their responsibilities.	• *Inspected* various job descriptions for Project positions. Inspected for the inclusion of required knowledge and experience.	No relevant exceptions noted.
	• *Obtained* and inspected the training curriculum for new hires and relevant continuing education.	No relevant exceptions noted.
	• *Tested* a sample of 29 of 688 employees verifying their passing exam scores for training classes where a test is required by the Project. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.4 Key systems and data have been inventoried and their owners identified.	• *Conducted* corroborative inquiries of the Director of Systems Administration and the Director of Programs regarding the process of inventorying and identifying system and data owners.	No relevant exceptions noted.
	• *Inspected* appropriate information systems documentation indicating key systems and their owners.	No relevant exceptions noted.
	• *Inspected* the organization chart and job descriptions for indication that individuals identified as key systems owners were positioned at appropriate levels within the Project.	No relevant exceptions noted.
1.5 Roles and responsibilities of the Project are defined, documented and understood.	• *Obtained* and *inspected* documentation for evidence roles and responsibilities within the Project are defined. The documentation inspected includes the following: ▪ organization chart, ▪ new hire orientation training records, and ▪ various job descriptions.	No relevant exceptions noted.
1.6 Personnel have sufficient authority to exercise the role and responsibility assigned to them.	• *Inspected* the organization chart to identify levels of authority.	No relevant exceptions noted.
	• *Conducted* corroborative inquiry of several staff regarding their authority to exercise the role and responsibilities assigned to them.	No relevant exceptions noted.
	• *Observed* staff members during the performance of their job duties.	No relevant exceptions noted.
	• *Inspected* various Project job descriptions for the following positions to provide evidence that they contained a definition of the appropriate authority levels.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.7 Personnel understand and accept their responsibility regarding internal control.	• *Inspected* copies of signed Confidentiality Agreements and Statements of Privacy Practices for employees selected in a sample.	No relevant exceptions noted.
	• *Conducted* corroborative inquiry of several staff members as to their acceptance and their responsibility regarding internal control.	No relevant exceptions noted.
	• *Observed* staff during the performance of their job duties noting conformity with the stated policies.	No relevant exceptions noted.
1.8 Management has implemented a division of roles and responsibilities (segregation of duties) that reasonably prevent a single individual from subverting a critical process.	• *Inspected* the organization chart and various job descriptions for appropriate segregation of duties.	No relevant exceptions noted.
	• *Observed* staff during the performance of their job duties for conformance with stated policies.	No relevant exceptions noted.
	• *Inspected* the Change Action Request (CAR) process and procedures for the appropriate segregation of duties and sign off procedures during the promotion of the code into production.	No relevant exceptions noted.
	• *Inquired* of the manager of software engineering as to the process of promoting code into production to verify the appropriate understanding and compliance with the CAR process and procedures.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.9 Staff evaluations are performed regularly. Employees receive their first written performance evaluation after 90 days of employment.	• *Obtained* completed performance evaluations for a sample of 29 of 688 employees to their Human Capital files. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%	No relevant exceptions noted.
	• *Inquired* of Human Capital personnel about the procedures and methodology of the evaluations performed.	No relevant exceptions noted.
1.10 All staff including contracted staff and other contract personnel are subject to policies and procedures created to control their activities by the IT function, and to assure the protection of the Project's information assets.	• *Inspected* a sample of 29 of 688 employee files for the existence of signed acknowledgement statements of privacy and practices. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%	No relevant exceptions noted.
	• *Inspected* the new hire procedures documentation for inclusion of the wording "pertains to: All contractors and temporary agencies staff."	No relevant exceptions noted.
	• *Inquired* of Human Capital management as to the procedure for obtaining new hire documentation and policy signatures.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.11 Significant IT events or failures, e.g., security breaches, major system failures or regulatory failures, are reported to senior management.	• *Inspected* procedural documentation for security alerts and monitoring control noting conformity with stated policy.	No relevant exceptions noted.
	• *Inquired* of the Technical Infrastructure Manager as to the procedures followed for this policy.	No relevant exceptions noted.
	• *Observed* the system monitoring screens and existing online reporting.	No relevant exceptions noted.
	• *Inspected* the Production Outage Report dated December 2009 containing cumulative reporting of production outages since June 8, 2006.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Management of Human Resources		
1.12 Controls are in place to support appropriate and timely responses to job changes and job terminations so that internal controls and security are not impaired by such occurrences.	• *Inspected* help desk logs indicating job changes, additions and deletions.	No relevant exceptions noted.
	• *Tested* the system access lists by comparing against the current employee lists to determine if any terminated employees still have access.	One (1) exception out of 3,235 active directory entries (.03%) was noted where a terminated employee's Active Directory account was not disabled. MAXIMUS Response: The termination request for this exception was received as a part of a consolidated ticket generated on December 31, 2009. However, one of the individual's Active Directory account was not properly disabled. Human Capital and IT HelpDesk dually manage this process. This single error out of 202 termination requests was discovered in the Systems' quarterly audit on March 10, 2010, a compensating control used to ensure 100% compliance. Research indicates the staff's duties did not include any need to log via the Active Directory before the termination. Problem Statement #66361 has been generated for corrective action plans to include generating individualized tickets for each termination request.
	• *Tested* the current application user IDs by comparing against the current employee lists to determine if any terminated employees still have access.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Educate and Train Users		
1.13 The Project subscribes to a philosophy of continuous learning, providing necessary training and skill development to its employees.	• *Inspected* a sample of the training records for selected staff (66 employees from a population of 688) for evidence of continuous training throughout their employment history. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%	No relevant exceptions noted.
	• *Inquired* of the Training Supervisor as to this policy indicating the provision for continuous learning, and providing necessary training and skill development to its members.	No relevant exceptions noted.
	• *Inspected* training materials for evidence of the variety of education courses and materials.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.14 Established procedures exist for identifying and documenting the training needs of all personnel that use information services in support of the Project.	• *Inspected* a sample of the training records (66 employees from a population of 688) for selected staff noting procedures for identifying and documenting training needs of all personnel. Parameters for the sample were: ▪ A 95% confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%	No relevant exceptions noted.
	• *Inquired* of the Training Supervisor as to the policies and procedures in place verifying conformity to the stated policy.	No relevant exceptions noted.
	• *Inspected* Quality Management System (QMS) documentation and training materials for evidence that education courses conform to the stated policy.	No relevant exceptions noted.
	• *Inspected* documentation of the security awareness training that is required for all new staff.	No relevant exceptions noted.
	• *Inspected* the employee manual and the Security and Confidentiality Policy for verification of conformity to the stated policy.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.15 Management provides education and ongoing training programs that include ethical conduct, system security practices, confidentiality standards, integrity standards and security responsibilities for all staff.	• *Inspected* various QMS documentation for evidence that both new employee and ongoing training is required.	No relevant exceptions noted.
	• *Traced* a sample of employees (29 out of 688) to their respective training records for completeness. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%	No relevant exceptions noted.
	• *Conducted* corroborative inquiry of the Director of Human Capital and the training management as to the procedures concerning education and ongoing training programs.	No relevant exceptions noted.
1.16 The Project has an activity-level risk assessment framework, which is used periodically to assess information risk for achieving business objectives, and it considers the probability and likelihood of threats.	• *Traced* a sample of four (4) statistics from the summary statistics (from the Key Performance Indicators report March 1, 2009 through February 28, 2010) to the source documents provided by the individual departments. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 1%. ▪ A sampling error rate of 10%.	No relevant exceptions noted.
	• *Inspected* the monthly Risk Assessment reports discussed in the tactical meetings for evidence of conformity with the stated policy.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.17 A user access audit is performed for critical systems and locations based on their relative priority and importance to the Project on a weekly basis.	• *Inquired* of Technology Infrastructure Manager as to the process of user audits for evidence of conformity with the stated policy. • *Tested* application user access rights by comparing to the current employee listing for differences.	No relevant exceptions noted. No relevant exceptions noted
1.18 Where risks are considered acceptable, there is formal documentation and acceptance of residual risk with related offsets, including adequate insurance coverage, contractually negotiated liabilities and self-insurance.	• *Inquired* of appropriate management personnel regarding the existence of formal documentation and acceptance of residual risk with related offsets, including adequate insurance coverage, contractually negotiated liabilities and self-insurance • *Obtained* and *inspected* the administrative contract with the MRMIB for inclusion of contractually negotiated liabilities and self-insurance.	No relevant exceptions noted. No relevant exceptions noted.
1.19 Access to the data center is restricted to authorized personnel, requiring appropriate identification and authentication.	• *Tested* data center access by attempting access using badges other than those that should be authorized. • *Inspected* data center visitor log for evidence of the dates, times, visitors, and the purposes of those visits. • *Inquired* of the Technical Infrastructure Manager about data center access policies and rules.	No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.20 A business impact assessment has been performed that considers the impact of systems failure on the case management process.	• *Inspected* the Business Impact Analysis prepared as part of the Business Continuity (BC) / Disaster Recovery (DR) plan for inclusion of the considerations of the impact of a systems failure, in the planning process.	No relevant exceptions noted.
Manage Facilities		
1.21 Facilities are adequately secured and managed.	• *Inquired* of the Facilities Coordinator regarding the management of security in the facility. • *Tested* current building badge access list against the active the active employee list for authorized badge holders. • *Tested* badge access by attempting access to inappropriate areas with various unauthorized badges and was refused access. • *Observed* that to obtain building access all employees and visitors must sign-in to the building in addition to wearing badges. Also noted that all visitors receive visitor badges. • *Observed* that a video surveillance system is operational in the building including a camera facing the server room door.	No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.22 Data center facilities are equipped with adequate environmental controls to maintain systems and data, including fire suppression, uninterrupted power service (UPS), generator, and appropriate air conditioning.	• *Conducted* corroborative inquiry of the Technical Infrastructure Manager and the Facilities Coordinator regarding the environmental controls in place. The responses indicated that the generator is tested by being run at full load once a year. There are also 15 minute test runs of the generator every Monday.	No relevant exceptions noted.
	• *Observed* the following environmental controls in the computer room: ▪ 20 ton Liebert air conditioner unit ▪ CATT generator with a 5,000 gallon fuel tank capacity ▪ fire rated door ▪ wet pipe sprinkler system ▪ battery backup for use during cut-over to the generator.	No relevant exceptions noted.
Compliance with External Requirements		
1.23 Control activities are in place and followed to ensure compliance with external requirements, such as regulatory and legal rules.	• *Inspected* various QMS documents for inclusion of control activities to ensure compliance with regulatory and legal requirements.	No relevant exceptions noted.
	• *Obtained* and *inspected* the California Healthy Families Performance Standards Analysis Report for evidence of the measurements of compliance.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Inspected* a sample of the personnel files (29 out of 688) and noted that appropriate confidentiality agreements (pertaining to HIPAA) are signed. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%	No relevant exceptions noted.
1.24 Internal events are considered in a timely manner to support continuous compliance with legal and regulatory requirements.	• *Inspected* various QMS documents for evidence that of support for continuous compliance with legal and regulatory requirements.	No relevant exceptions noted.
	• *Obtained* and *inspected* the California Healthy Families Performance Standards Analysis Report.	No relevant exceptions noted.
	• *Inquired* of appropriate management that contract requirements are monitored regularly by management.	No relevant exceptions noted.
Management of Quality		
1.25 Documentation is created and maintained for all significant processes, controls and activities.	• *Obtained* and *inspected* various QMS documentation for evidence of a maintenance cycle including appropriate revision dates. Also inspected the electronic document properties for evidence that the documents are being maintained.	No relevant exceptions noted.
	• *Inspected* minutes of the IPWG meeting where the documents are approved.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.26 A plan exists to maintain the overall quality assurance of activities, based on the Project plans.	• *Inspected* the Quality Manual and QMS Plan for evidence of assurance activity in the project.	No relevant exceptions noted.
	• *Inquired* of management in the QA department as to the plan to maintain the quality assurance activities for the Project.	No relevant exceptions noted.
1.27 Documentation standards are in place and have been communicated to all staff, and are supported with training.	• *Obtained* and *inspected* QMS documentation for evidence that documentation standards are in place.	No relevant exceptions noted.
	• *Inquired* of the Training Department management that standards do exist and are: ▪ in place, ▪ communicated to all staff, and ▪ supported with training.	No relevant exceptions noted.
	• *Inspected* various Work Instructions (WI) documents for evidence of appropriate process documentation.	No relevant exceptions noted.
1.28 A quality plan exists for significant IT functions (e.g., large system development and deployment projects) and it provides a consistent approach to address both general and project-specific quality assurance activities.	• *Inspected* documentation for the existence of the inclusion of a QA process contained in significant IT functions. The documentation included: ▪ QA audit reports for the year, ▪ CA HFP Quality Manual, and ▪ ISO 9000 Internal Quality Audit.	No relevant exceptions noted.
	• *Inspected* four (4) of the twelve (12) monthly MQMPR reports performed during the year to assure the existence of general and project specific assurance activities.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	- *Inquired* of QA management as to their involvement in CAR Projects to verify a consistent approach is being used in the testing of any CARs prior to deployment into production.	No relevant exceptions noted.
1.29 The quality plan prescribes the type(s) of quality assurance activities (such as reviews, audits, inspections) to be performed to achieve the objectives of the quality plan.	- *Inspected* the document CA HFP Quality Manual to determine if it prescribes the type(s) of quality assurance activities (such as reviews, audits, inspections) to be performed.	No relevant exceptions noted.
1.30 The quality assurance process includes a review of adherence to policies, procedures and standards.	- *Inspected* documentation for the existence of the review and adherence to procedures and standards. The documentation inspected included the: ▪ CA HFP Quality Manual, ▪ ISO 9000 Internal Quality Audit, and ▪ Corporate QA Best Practices Checklist.	No relevant exceptions noted.
	- *Inquired* of the Quality Assurance Director as to the quality assurance process and review of adherence to the policies and procedures.	No relevant exceptions noted.
	- *Inspected* reports that alert managers regarding procedure or work instruction review for the adherence to the policies, procedures and work instructions.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Manage Performance and Capacity		
1.31 IT management monitors the performance and capacity levels of the systems and network.	• *Inquired* of the Technical Infrastructure Manager as to the procedure in place to monitor performance and capacity of the systems and the network.	No relevant exceptions noted.
	• *Observed* onscreen reporting and trends provided by Nagios for completeness and evidence of the inclusion of capacity levels.	No relevant exceptions noted.
1.32 IT management has a process in place to respond to suboptimal performance and capacity measures.	• *Inspected* a sample of 72 of 6880 helpdesk entries noting that suboptimal performance and capacity measures were properly logged and resolved. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 5%. ▪ A sampling error rate of 5%	No relevant exceptions noted.
	• *Inspected* a completed Management Review Packet that was presented to upper management.	No relevant exceptions noted.
	• *Inquired* of management as to the procedure used to respond to suboptimal performance or capacity issues.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.33 Performance and capacity planning is included in system design and implementation activities.	• *Inspected* a sample of 27 of 238 CARs in all status levels for the examination period. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5% For each CAR in the sample, inspected the performance impact analysis documents for all relevant CARs.	No relevant exceptions noted.
	• *Inquired* of the Software Engineering Manager concerning: ▪ scheduling of the implementations ▪ impact analysis process ▪ peer review and code performance.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.34 Performance indicators or benchmarks, from both internal and external sources, have been defined, and data is collected and reported regarding achievement of these benchmarks.	• *Inspected* documentation for the existence of the use of internal and external benchmarks. The documentation inspected included: ▪ CHFP Performance Standards Report, ▪ Weekly Risk Assessment Reports, ▪ Call Center Report, ▪ Weekly and Monthly Administrative Vendor Reports, and ▪ Project Status Report.	No relevant exceptions noted.
	• *Obtained* and *inspected* a sample of four (4) statistics from the summary statistics (from the Key Performance Indicators report March 1, 2009 through February 28, 2010). Compared the statistics reported to the source documents provided by the individual departments for accuracy. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 1%. ▪ A sampling error rate of 10%.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.35 Management has established appropriate metrics to effectively manage the day-to-day activities.	• *Inspected* documentation for evidence of the use of metrics by the management staff. The documentation inspected included: ▪ CHFP Performance Standards Report, ▪ Weekly Risk Assessment Reports, ▪ Call Center Report, ▪ Weekly and Monthly Administrative Vendor Reports, and ▪ Project Status Report.	No relevant exceptions noted.
	• *Obtained* and *inspected* a sample of four (4) statistics from the summary statistics (from the Key Performance Indicators report March 1, 2009 through February 28, 2010). Compared the statistics reported to the source documents provided by the individual departments for accuracy. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 1%. ▪ A sampling error rate of 10%.	No relevant exceptions noted.
	• *Conducted* corroborative inquiry of the Deputy Project Manager, the Financial Operations Director, and the Human Capital Director regarding the use of metrics to manage their department.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.36 Management monitors delivery of services to identify shortfalls and responds with actionable plans to improve.	• *Inspected* documentation for evidence of the use and monitoring of specific performance measurements. The documentation inspected included: ▪ CHFP Performance Standards Report, ▪ Weekly Risk Assessment Reports, ▪ Call Center Report, ▪ Weekly and Monthly Administrative Vendor Reports, and ▪ Project Status Report.	No relevant exceptions noted.
	• *Inquired* of QA management as to the procedures and practices that are performed to monitor, identify and improve on services performed.	No relevant exceptions noted.
Management of Internal Control		
1.37 Management monitors the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons and benchmarks.	• *Conducted* corroborative inquiry of the Deputy Project Manager, the Financial Operations Director, and the Human Capital Director regarding the monitoring and effectiveness of internal controls.	No relevant exceptions noted.
1.38 Serious deviations in the operation of internal control, including major security, availability and processing integrity events, are reported to senior management.	• *Inquired* of the Director of Information Systems and discussed the procedures of informing management of deviations in the operation of internal control, including major security, availability and processing integrity events.	No relevant exceptions noted.
	• *Inspected* the Production Outage Report dated December 2009 containing cumulative reporting of production outages since June 8, 2006.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Inspected* documentation for the inclusion of the resolution of serious deviations in operations. The documentation inspected included: ▪ the Mercury ITG logs, ▪ the CAR logs, and ▪ meeting minutes discussing problem statements and CARS.	No relevant exceptions noted.
1.39 Internal control assessments are performed periodically, using self-assessments, to examine whether or not internal controls are operating satisfactorily.	• *Inquired* of appropriate management and discussed the procedures and practices in place to examine if internal controls are operating satisfactorily.	No relevant exceptions noted.
	• *Inspected* the Production Outage Report dated December 2009 containing cumulative reporting of production outages since June 8, 2006.	No relevant exceptions noted.
	• *Inspected* various documentation that would include an indication of internal control deviations including but not limited to: ▪ the Mercury ITG logs, ▪ the CAR logs, ▪ meeting minutes discussing problem statements and CARS, ▪ Risk Assessment reports, ▪ QA inspections reports, and ▪ management review meeting minutes.	No relevant exceptions noted.

Controls Specified by MAXIMUS		
1.40 Internal Audit engagements are performed based on approval by the audit committee.	• *Inspected* the various internal audit reports for the inclusion of review and approval by the audit committee. • *Inspected* the approved schedule of internal audits for the existence of approval by the audit committee. • *Compared* internal audit reports against approved schedule of Internal Audits for the existence of adherence to the schedule and content.	No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted.
1.41 A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.	• *Inspected* the Supplier / Subcontractor Performance Standards Analysis Report for compliance with the control. • *Inspected* the QMS document Subcontractor Supplier Approval for verification of a formalized process for subcontractor/supplier approval. • *Inquired* of the Contracts Manager as to the procedures in place to monitor the third-party service level performance criteria.	No relevant exceptions noted. No relevant exception noted. No relevant exception noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.42 The selection of vendors for outsourced services is performed in accordance with the Project's vendor management policy.	• *Inquired* of the Contract Compliance Manager that the Project complies with the Authority and Responsibility Policies and Procedures Manual. The Contract Compliance Manager stated the policies require evaluation criteria consider that during solicitation planning and due diligence a minimum of three written competitive quotations are obtained.	No relevant exceptions noted.
	• *Inspected* documentation for evidence of the Project's vendor management policy. The documents inspected included: ▪ Authority and Responsibility Policies and Procedures Manual, ▪ Vendor contracts and compliance matrix with outsource vendors, and ▪ Subcontractor supplier approval.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.43 Before selection, management determines that potential third parties are properly qualified through an assessment of their capability to deliver the required service.	• *Inquired* of the Contract Compliance Manager regarding the Project's use of an RFP process to review the qualifications of vendors prior to their being contracted to perform services. In addition, the inquiry of the Contract Compliance Manager was meant to verify that potential vendors are assessed, exceptions to subcontractor agreement packages are evaluated and financial impact reviews are performed for Executive Management.	No relevant exceptions noted.
	• *Obtained* and *inspected* the documented policy on Subcontractor Approval which provides guidelines for: ▪ The maintenance of the HFP subcontracts through amendments and clarifications. ▪ Ensuing adherence and retention of the HFP Prime Contract through the evaluation of Subcontractors. ▪ The negotiation and award of subcontracts under the HFP Prime Contract. ▪ The record of contract negotiations, contract review, amendments, and clarifications.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.44 Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.	• *Inspected* the existing vendor contracts with outsource vendors for the inclusion of identified risks and security controls.	No relevant exceptions noted.
	• *Obtained* and *inspected* the documented policy on Subcontractor Approval which provides guidelines for: ▪ Maintenance of the CA HFP Sub-Contracts through amendments and clarifications. ▪ Ensuing adherence and retention of the CA HFP Prime Contract through the evaluation of Subcontractors. ▪ Negotiation and award of Subcontracts under the CA HFP Prime Contract. ▪ Record of contract negotiations, contract review, amendments, and clarifications.	No relevant exceptions noted.
	• *Inquired* of the appropriate management personnel, as to the existence of risks, security controls and procedures for information systems and networks in the contract between the parties within the third-party service contracts.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.45 Procedures exist and are followed to ensure that a formal contract is defined and agreed for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the Project's policies and procedures.	• *Inquired* of the appropriate management personnel to verify that the project complies with the Authority and Responsibility Policies and Procedures Manual. • *Inspected* documentation to verify that procedures exist to ensure that a formal contract is defined and agreed to for all third-party services before work is initiated. The documentation inspected included but was not limited to: ▪ Authority and Responsibility Policies and Procedures Manual ▪ Vendor Contracts and Compliance Matrix with Outsource Vendors ▪ Subcontractor Supplier Approval	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
1.46 A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.	• *Inquired* of the appropriate management personnel as to the procedures in place to review the security, availability and processing integrity for service level agreements.	No relevant exceptions noted.
	• *Inspected* Subcontractor Supplier Approval assuring that it provides guidelines for: ▪ Maintenance of the Subcontracts via amendments and clarifications. ▪ Ensuing adherence and retention of the Prime Contract through the evaluation of Subcontractors. ▪ Negotiation and award of Subcontracts under the Prime Contract. ▪ Record of contract negotiations, contract review, amendments, and clarifications.	No relevant exceptions noted.
	• *Inspected* the vendor contracts and compliance matrix with third-party service providers for the existence of a regular review of security, availability and processing integrity.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Computer Operations Controls		
Control Objective 2: Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved, or investigated for proper resolution.		
2.1 IT management has defined and implemented a problem management system to ensure that operational events (breakage, problems, and errors) not part of the standard operation, are recorded, analyzed, and resolved in a timely manner.	• *Inquired* of Helpdesk employees as to the policies and procedures in place noting conformity with stated policy. • *Inspected* a sample of 72 of 6880 helpdesk entries from entry to resolution and obtained proof of resolution, as well as noting the resolution was performed in a timely manner where available. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 5%. ▪ A sampling error rate of 5%	No relevant exceptions noted. One (1) exception with thirteen (13) instances was noted for the Helpdesk tickets: two (2) instances where proof of a resolution was not found. 2.78% error rate; and eleven (11) instances where proof of a timely resolution was not met. 15.28% error rate. MAXIMUS Response: These HelpDesk ticket instances are jointly generated from both the Facilities and Information Systems Departments, four (4) and nine (9), respectively. In most cases, the tickets needed additional help from external resources, which delayed the timely closure of the tickets. In two (2) cases involving Facilities tickets with low priority status, the tickets were closed without sufficient notation of details and conclusion. Problem Statement #66360 has been generated for a staff training refresher and preventive action plans, which include the implementation of enhanced exception report monitoring as well as evaluating the effectiveness of the procedures to improve performance.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
2.2 The problem management system provides for adequate audit trail facilities, which allow tracing from incident to underlying cause.	• *Inquired* of Helpdesk employees as to the policies and procedures in place for the existence of a problem management system.	No relevant exceptions noted.
	• *Inspected* a sample of 72 of 6880 helpdesk entries from entry to resolution and inspecting proof of resolution when available. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 5% (appropriate sample size). ▪ A sampling error rate of 5%.	There were two (2) instances (see finding under 2.1 above) where proof of a resolution was not found. 2.78% error rate. MAXIMUS Response: These HelpDesk ticket instances are jointly generated from both the Facilities and Information Systems Departments, four (4) and nine (9), respectively. In most cases, the tickets needed additional help from external resources, which delayed the timely closure of the tickets. In two (2) cases involving Facilities tickets with low priority status, the tickets were closed without sufficient notation of details and conclusion. Problem Statement #66360 has been generated for a staff training refresher and preventive action plans, which include the implementation of enhanced exception report monitoring as well as evaluating the effectiveness of the procedures to improve performance.
2.3 A security incident response process exists to support timely response and investigation of unauthorized activities.	• *Inquired* of Helpdesk employees as to the policies and procedures in place noting conformity with stated policy.	No relevant exceptions noted.
	• *Inspected* Helpdesk processes and procedures related to security incident response.	No relevant exceptions noted.
	• *Inquired* of IT management regarding the involvement of the Information Security Administrator in responding to a security incident.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
2.4 A contingency plan has been developed for alternative processing in the event of loss or interruption of the IT function.	• *Inspected* the Contingency Plan BC / DR plan noting the inclusion of alternative processing.	No relevant exceptions noted.
	• *Inquired* as to the feasibility of the BC / DR plan with the Director of Information Services.	No relevant exceptions noted.
Control Objective 3: Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.		
3.1 Policies and procedures exist for the handling, distribution and retention of data and reporting output.	• *Inspected* documentation for evidence of the existence of procedures for the handling, distribution, and retention of data. The documentation inspected included the following: ▪ MAXIMUS Information Security Policy, ▪ Security and confidentiality policy, and ▪ Backup and offsite storage procedures.	No relevant exceptions noted.
	• *Inquired* of the Technical Infrastructure Manager confirming the following: ▪ All files sent to vendors are transported by secure courier. ▪ Backup and storage files are transported by secure courier. ▪ All files distributed outside the Project are either encrypted or transported by a secure courier.	No relevant exceptions noted.
	• *Inspected* the following for the inclusion of proper handling of data: ▪ public certificates for all vendors where data is shared electronically. ▪ Inspected a nightly file transfer log utilizing the public certificates.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
3.2 Management protects sensitive information, logically and physically, in storage and during transmission against unauthorized access or modification.	• *Inquired* of the Technical Infrastructure Manager to verify the following elements are in use: ▪ All files sent to vendors are transported by secure courier. ▪ Backup and storage files are transported by secure courier. ▪ All files distributed outside the project are either encrypted or transported by a secure courier. ▪ Virus protection is active on all desktops. ▪ User areas of the network are segregated by VLANs and firewalls.	No relevant exceptions noted.
	• *Inspected* evidence of: ▪ public certificates for all vendors where data is shared electronically, and ▪ a nightly file transfer log utilizing the public certificates.	No relevant exceptions noted.
3.3 Retention periods and storage terms are defined for documents, data, programs, reports and messages (incoming and outgoing), as well as the data (keys, certificates) used for their encryption and authentication.	• *Inspected* the contract with the MRMIB, for the existence of defined retention periods.	No relevant exceptions noted.
	• *Inquired* of the Technology Infrastructure Manager: ▪ retention periods for electronic information ▪ noted that electronic data is retained in perpetuity	No relevant exceptions noted.
	• *Observed* the hardcopy file room area and procedures, noting evidence that policies and procedures exist for the handling, distribution and retention of data and reporting output.	No relevant exceptions noted. .

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
3.4 Management has implemented a strategy for cyclical backup of data and programs.	• *Inspected* PP-17-18, CAHFP Data Backup Procedures for the inclusion of a backup strategy.	No relevant exceptions noted.
	• *Inquired of* the Technical Infrastructure Manger regarding the cyclical backup schedule.	No relevant exceptions noted.
3.5 Procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media.	• *Inspected* PP-17-18 CAHFP Data Backup Procedures for the existence of testing procedures.	No relevant exceptions noted.
	• *Inquired* of the Technical Infrastructure Manager regarding the test procedures for performing restorations. Noted that they are performed regularly in addition to full database restorations which are used to refresh the development and reporting environments.	No relevant exceptions noted.
	• *Inspected* a copy of a recent tape inventory audit of the off-site vendor by IS personnel for the existence of regular tape inventories.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
3.6 Changes to data structures are authorized, made in accordance with design specifications, and implemented in a timely manner.	• *Inspected* the following: ▪ PP-12-01 – Corrective and Preventive Action ▪ PP-17-10 – System Code Migration Procedure ▪ PP-17-23 – Change Action Request (CAR) for the existence of change authorization.	No relevant exceptions noted.
	• *Inquired* of the Manager of Software Engineering regarding the: ▪ promotion process for authorized changes to data structures and results ▪ DBA role in promotions ▪ testing and validating data and reports.	No relevant exceptions noted.
	• *Inspected* a sample of CARs (27 of 238) to validate testing, approval, and promotion of authorized changes. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%	No relevant exceptions noted.
Control Objective 4: Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring, and system availability.		
4.1 Management has established and documented standard procedures for IT operations, including scheduling, managing, monitoring and responding to security, availability, and processing integrity events.	• *Inspected* the ticket handling documents and documentation for completeness noting conformity to stated policy.	No relevant exceptions noted.
	• *Inquired* of the appropriate IT management regarding policies and procedures that address documentation standards for IT operations.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
4.2 System event data is sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of system and data processing.	• *Inquired* of the level two Helpdesk Technician as to this process. • *Inspected* a sample of server logs from the period under review.	No relevant exceptions noted. No relevant exceptions noted.
4.3 System event data is designed to provide reasonable assurance as to the completeness and timeliness of system and data processing.	• *Inquired* of management as to the process in place to obtain assurance as to the completeness and timeliness of system and data processing. • *Observed* notifications of processing results for important processing.	No relevant exceptions noted. No relevant exceptions noted.
4.4 Policies and procedures are followed concerning security, availability and processing integrity for packaged software products that are purchased for end-user computing.	• *Inspected* the Client Image Testing Checklist for completeness for the existence of security identification in the packaged software. • *Observed* that installation files are kept in a secure directory and physical install disks are kept in a locked box in a locked room. • *Inquired* of the Manager of Software Engineering as to the procedures for testing end user software products to verify compatibility with existing systems.	No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted.
4.5 User-developed systems, such as spreadsheets and other end-user programs, are secured from unauthorized use.	• *Inspected* CP-02 - Security and Confidentiality Policy, noting the inclusion of security of end-user programs. • *Conducted* corroborative inquiry of the Technical Infrastructure Manager and IS Director as to the security of user developed systems.	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
4.6 Access to user-developed systems is restricted to an authorized and limited number of users.	• *Inspected* CP-02 - Security and Confidentiality Policy for the inclusion of restricted access to user-developed systems. • *Conducted* corroborative inquiry of the Technical Infrastructure Manager and IS Director regarding security of user developed systems.	No relevant exceptions noted. No relevant exceptions noted.
Security and Access Controls		
Control Objective 5: Controls provide reasonable assurance that Project information technology (IT) operating systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage, or loss of data.		
5.1 An information security policy and framework exists and has been approved by an appropriate level of executive management.	• *Inspected* the following: ▪ CP-02 Security and Confidentiality Policy. Inspected the Revision History section noting that it is maintained on a regular basis. ▪ The MAXIMUS Information Security Policy. for the existence of regular updates and executive management approval of the policies.	No relevant exceptions noted.
5.2 Procedures exist and are followed to authenticate all users to the system to support the validity of transactions.	• *Inspected* the roles and access lists for the system and Oracle Financials for the existence of authentication to the software. • *Inquired* of the appropriate IT management regarding user authentication controls, as well as ensuring the validity of access rights and transaction validation.	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
5.3 Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes).	• *Inspected* the MAXIMUS Information Security Policy for the inclusion of authentication mechanisms.	No relevant exceptions noted.
	• *Inspected* CP-02 - Security and Confidentiality Policy for the inclusion of authentication mechanisms.	No relevant exceptions noted.
	• *Inquired* of the Infrastructure Services Manager about the authentication and access mechanisms in the Information Security Policy.	No relevant exceptions noted.
	• *Tested* the active directory LDAP to assure that only special accounts with limited access capability are set never to expire. The testing made use of computer assisted tools to download the LDAP and probe it for accounts that never expire.	No relevant exceptions noted.
5.4 Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts.	• *Inquired* of level two helpdesk technician as to these procedures for timely action relating to user accounts.	No relevant exceptions noted.
	• *Inspected* PP-17-12 – User Add/Delete defining the process of adding or deleting a user from the system.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
5.5 A control process exists and is followed to periodically review and confirm access rights.	• *Inquired* of the Technical Infrastructure Manager regarding the periodic process of reviewing the terminations list to assure that terminated staff is no longer provided system access.	No relevant exceptions noted.
	• *Tested* the system access lists using computer assisted audit tools to download the current list of active users, and then compared the list against the current employee list to determine if any terminated employees still have access.	One (1) exception out of 3,235 active directory entries (.03%) was noted where a terminated employee's Active Directory account was not disabled. MAXIMUS Response: The termination request for this exception was received as a part of a consolidated ticket generated on December 31, 2009. However, one of the individual’s Active Directory account was not properly disabled. Human Capital and IT HelpDesk dually manage this process. This single error out of 202 termination requests was discovered in the Systems’ quarterly audit on March 10, 2010, a compensating control used to ensure 100% compliance. Research indicates the staff’s duties did not include any need to log via the Active Directory before the termination. Problem Statement #66361 has been generated for corrective action plans to include generating individualized tickets for each termination request.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
5.6 Where network connectivity is used appropriate controls, including the use of firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access.	• *Inspected* the CAHFP network diagram for protective design and the inclusion of protective devices.	No relevant exceptions noted.
	• *Inquired* of the Technical Infrastructure Manager regarding: ▪ network configuration ▪ controls used to prevent unauthorized access ▪ use of Nessus on new servers prior to implementation.	No relevant exceptions noted.
	• *Inspected* the results of a recent external vulnerability scan for the existence of existing vulnerabilities and resolutions.	No relevant exceptions noted.
5.7 IT security administration monitors and logs security activity, and identifies and reports security violations to senior management.	• *Inquired* of Corporate Network personnel regarding network security monitoring.	No relevant exceptions noted.
	• *Inspected* scan results against the network perimeter.	No relevant exceptions noted.
5.8 Appropriate segregation of duties over requesting and granting access to systems and data exists and is followed.	• *Inquired* of the Technical Infrastructure Manager for verification that Human Capital requests the user access accounts via the helpdesk process. IS personnel create the accounts requested by Human Capital.	No relevant exceptions noted.
	• *Inspected* - IT organization chart for the existence of appropriate segregation of duties.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
5.9 Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication.	• *Inquired* of the Facilities Coordinator for verification of the facility access policy.	No relevant exceptions noted.
	• *Observed* the facilities access at the entry point to the building for verification that the building has a locked entry point controlled by the receptionist All visitors must present an ID and be escorted throughout the facilities.	No relevant exceptions noted.
	• *Inspected* documentation and procedures that define restricted access to the facilities. The documents inspected include: ▪ CP-02 Security and Confidentiality Policy ▪ PP-17-02 Data Center Policies and Procedures ▪ Facilities Access Log	No relevant exceptions noted.
Control Objective 6: Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.		
6.1 Only authorized software is permitted for use by employees using Project IT assets.	• *Inspected* the MAXIMUS Information Security Policy for evidence of restrictions for the use of authorized software only.	No relevant exceptions noted.
	• *Inquired* of the Technical Infrastructure Manager regarding the practice of performing an automated software inventory periodically to identify unauthorized applications. In addition, also inquired as to the group policy in place to prohibit personnel from installing applications on their individual machines.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
6.2 Application software and data storage systems are properly configured to provide access based on the individual's job responsibilities.	• *Tested* the system access lists using computer assisted audit tools to download the current list of active users, and then compared the list against the current employee list to determine if any terminated employees still have access.	No relevant exceptions noted.
	• *Inquired* of the Technical Infrastructure Manager regarding data storage and system access.	No relevant exceptions noted.
	• *Inspected* a sample selection of users and their access roles and confirmed the access roles were commensurate with the job responsibilities with appropriate management personnel.	No relevant exceptions noted.
6.3 IT management has established and implemented procedures and security tools across the project to protect information systems and technology from computer viruses.	• *Conducted* corroborative inquiry of the Technical Infrastructure Manager and IS Director regarding the information systems virus protection policies. Inquires were meant to confirm that: ▪ virus protection exists at several layers of the network, ▪ virus protection exists at the desktop, and ▪ virus protection exists for email.	No relevant exceptions noted.
	• *Observed* workstation compliance with the procedures that are established to protect the Project from computer viruses.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
6.4 Periodic testing and assessment is performed to confirm that software and the network infrastructure is appropriately configured.	• *Inquired* of the Infrastructure Manager as to the procedures in place to confirm that software and network infrastructure is appropriately configured, including the weekly review process, and monitoring using Nagios open source computer system and network monitoring application. • *Observed* onscreen reporting and trends provided by Nagios. • *Inspected* the results of the periodic vulnerability tests from the March 1, 2009 to February 28, 2010 time period.	No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted.
Acquisition, Development and Change		
Control Objective 7: Controls provide reasonable assurance that technology infrastructure is acquired to provide the appropriate platforms to support case management operating applications.		
7.1 Documented procedures exist and are followed to ensure that infrastructure systems, including network devices and software, are acquired based on the requirements of the case management applications they are intended to support.	• *Inspected* Infrastructure Change Control Procedures for the inclusion of change control and testing of changes. • *Conducted* corroborative inquiry of the infrastructure change process with the Director of Information Systems and the Technical Infrastructure Manager.	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 8: Controls provide reasonable assurance that application software is acquired or developed to effectively support both the California Healthy Families program and the Access for Infants and Mothers program case management operating requirements.		
8.1 The Project's acquisition and planning process ensures that infrastructure modifications are aligned with client the Project's specifications.	• *Inspected* PP-17-23 Change Action Request (CAR) for the inclusion of an infrastructure acquisition and planning process. • *Conducted* corroborative inquiry as to the infrastructure acquisition and planning process with the Director of Information Systems and the Technical Infrastructure Manager.	No relevant exceptions noted. No relevant exceptions noted.
8.2 IT management ensures that users are appropriately involved in the design of applications, selection of packaged software and the testing thereof, to ensure a reliable environment.	• *Inspected* PP-17-23 Change Action Request (CAR) for the inclusion of IT management and users in the CAR process. • *Conducted* corroborative inquiry as to the CAR process with the Director of Information Systems and the Technical Infrastructure Manager.	No relevant exceptions noted. No relevant exceptions noted.
8.3 IT management ensures that information systems are designed to include application controls that support complete, accurate, authorized, and valid transaction processing.	• *Inspected* the Project's Quality Management System documentation for the inclusion of controls around valid transaction processing. • *Inquired* of IT management as to the procedures in place to ensure that information systems are designed to include application controls to support complete, accurate, authorized, and valid transaction processing.	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
8.4 Post-implementation reviews are performed to verify controls are operating effectively.	• *Conducted* corroborative inquiry of the IS Application Development Manager and the Systems Analysis Manager regarding the control verification in the post-implementation review process. • *Inspected* the CARs in Closed and Post-Implementation Review status for evidence that post implementation reviews are performed.	No relevant exceptions noted. No relevant exceptions noted.
Control Objective 9: Controls provide reasonable assurance that systems are appropriately tested and validated prior to being placed into the production processing environment, and that associated controls operate as intended to support the case management operating requirements.		
9.1 A testing strategy was developed and implemented in January 2006 and followed for all significant changes in applications and infrastructure technology, which addresses unit-, system-, integration- and user acceptance-level testing to help ensure that deployed systems operate as intended subsequent to that time.	• *Inspected* PP-17-23 – Change Action Request for the definition and controls used in the testing strategy. • *Sampled* the CAR database and traced the relevant CARS back to the source documents to verify the compliance to the defined testing process. ▪ A random sample of thirty (30) CARS were selected from the CARS entered during the examination period. ▪ A review of the test scripts and results was completed for all relevant CARS selected in the random sample.	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
9.2 Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid.	• *Obtained* and *inspected* cash receipts from a sample of dates for: ▪ Aquracy – HFP (62), AIM (61) ▪ Credit Card (36) ▪ EFT (all months) ▪ Western Union (61) Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%.	No relevant exceptions noted.
	• *Tested* to verify that the batch totals transferred agreed to the file total, then traced to the posting in Oracle Financials (for both HFP and AIM).	No relevant exceptions noted.
9.3 The conversion of data is tested between its origin and its destination to confirm that it is complete, accurate and valid.	• *Inspected* the batch control totals for the sample of import files for: ▪ Aquracy HFP (62), AIM (61) ▪ Credit Card (36) ▪ EFT (all months) ▪ Western Union (61)	No relevant exceptions noted.
	• *Tested* the footed file totals by tracing them to the batch footer for the sample selected. Traced the total posted to the general ledger to the total in the batch footer for the sample selected.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 10: Controls provide reasonable assurance that policies and procedures defining required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.		
10.1 Policies and procedures have been created for the development of system specifications.	• *Inspected* documentation for the existence of policies and procedures governing the development of system specifications. The documentation inspected included the following: ▪ PP-10-05 – Handling and Control of Fast Alerts and Program Alerts, ▪ PP-12-01 – Corrective and Preventive Action, ▪ PP-17-00 – Information Systems Department Overview, ▪ PP-17-23 – Change Action Request (CAR), ▪ WI-17-10-01 – System Code Migration Procedure.	No relevant exceptions noted.
10.2 System development policies and procedures are regularly reviewed, updated, and approved by management.	• *Inspected* documentation for evidence that all policies, procedures and work instructions are inspected, updated and approved at least every six months via the Key Process Review Procedure. The documentation inspected included the following: ▪ PP-12-02 – ISO 9000 Internal Quality Audits, ▪ PP-12-09 – Key Process Reviews, and ▪ PP-10-01 – Document Creation and Control.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Conducted* corroborative inquiry of the Training Manager and the Director of QA regarding the: ▪ policy and procedure review process, and ▪ the reporting and tracking of the policy and procedure update process.	No relevant exceptions noted.
10.3 Project management ensures that its systems and applications are developed in accordance with supported, documented policies and procedures.	• *Inspected* documentation for the inclusion of development procedures and processes. The documentation inspected included the following: ▪ PP-10-05 – Handling and Control of Fast Alerts and Program Alerts, ▪ PP-12-01 – Corrective and Preventive Action, ▪ PP-17-00 – Information Systems, Department Overview, ▪ PP-17-23 – Change Action Request (CAR), and ▪ WI-17-10-01 – System Code Migration Procedure.	No relevant exceptions noted.
	• *Inspected* a sample of 27 CARs from a population of 238 that were created during the examination period. The sample was tested through the respective processes for evidence of compliance with the appropriate policies and procedures.	No relevant exceptions noted.
	• *Inquired* of appropriate management regarding policies and procedures that govern systems and application development efforts.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 11: Controls provide reasonable assurance that system changes of operational significance are appropriately tested and authorized before movement into production.		
11.1 Requests for program changes, system changes and maintenance (including changes to system software) are standardized documented and subject to formal change management procedures.	• *Inspected* documentation for the existence of formal change management procedures. The following documentation was inspected: ▪ PP-17-23 – Change Action Request (CAR), ▪ PP-12-09 – Key Process Reviews, ▪ PP-12-01 – Corrective and Preventive Action, and ▪ WI-17-10-01 – System Code Migration Procedure.	No relevant exceptions noted.
	• *Conducted* corroborative inquiry of the Application development Manager and the Director of QA regarding the use of formal documentation and change management procedures.	No relevant exceptions noted.
	• *Inspected* a sample of 27 CARs for the use of a formalized change management procedure. The sample was drawn from a population of 238 CARs from the examination period. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
11.2 Emergency change requests are documented and subject to formal change management procedures.	• *Inspected* documentation for evidence of the inclusion of formalized emergency change procedures. The documentation examined included the following: ▪ PP-10-05 – Handling and Control of Fast Alerts and Program Alerts, and ▪ PP-17-23 – Change Action Request (CAR).	No relevant exceptions noted.
	• *Inquired* of the Application Development Manager regarding the emergency change process.	No relevant exceptions noted.
11.3 Controls are in place to restrict migration of programs to production only by authorized individuals.	• *Inspected* documentation for evidence of the inclusion of controls around a formalized migration of programs. The documentation inspected included the following: ▪ PP-17-10 – System Code Migration Procedure, and ▪ WI-17-10-01 – System Code Migration Procedure.	No relevant exceptions noted.
	• *Inquired* of the Application Development Manager regarding the process of migrating applications to production.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
11.4 IT Management ensures that setup and implementation of system software do not jeopardize the security of the data and programs being stored on the system.	• *Conducted* corroborative inquiry of the System Development Manager and the Oracle and the system Database Administrators (DBAs) regarding the security of data during system implementations.	No relevant exceptions noted.
	• *Inspected* a sample of 27 CARs from a population of 238 that were created during the examination period. The sample was tested through the respective processes for evidence of compliance with the appropriate policies and procedures.	No relevant exceptions noted.
Application Processing Controls – Case Management Systems		
Control Objective 12: Input controls provide reasonable assurance that: • Originating HFP and AIM source data enters into the system through trained and authorized persons, and that data preparation procedures are established and followed to minimize errors and omissions, and to allow the input of only valid data into the system. • Authorized source documentation and data is complete and accurate, properly accounted for, and transmitted in a timely manner. • Error handling procedures detect errors and irregularities and report them for corrective action. • Source documents are retained and available for reconstruction and legal compliance.		
12.1 Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive appropriate procedure training for their job responsibilities.	• *Obtained* and *inspected* documentation for evidence of training requirements. The documentation included the following: ▪ PP-03-01 – SPE Data Entry, ▪ PP-05-02 – Case Correction Request, ▪ WI-02-02-02 – Initial Receipt and Determination, and ▪ WI-02-02-01 – Missing Info for HFP Apps.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Conducted* corroborative inquires with the Mail Room Manager and Manager of Enrollment and Eligibility regarding the use of documented procedures, work instructions and training procedures related to input controls.	No relevant exceptions noted.
	• *Obtained* and *inspected* the training curriculum for new hires and continuing education for the inclusion of procedure and work instruction training.	No relevant exceptions noted.
	• *Tested* a sample of 29 of 688 employees for proper testing by inspecting evidence of passing exam scores for training.	No relevant exceptions noted.
12.2 Personnel are organized by function and provided access to information systems in terms of job responsibilities. Critical input functions are separate from critical processing functions. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Obtained* and *inspected* documentation for evidence of segregation of critical functions. The following documentation was inspected: ▪ PP-03-01 – SPE Data Entry, ▪ PP-05-02 – Case Correction Request, ▪ WI-02-02-02 – Initial Receipt and Determination, and ▪ WI-02-02-01 – Missing Info for HFP Apps.	No relevant exceptions noted.
	• *Observed* the data entry and review process for all levels according to the workflow in PP-03-01 – SPE Data Entry for evidence of the separation of critical functions and adherence to policies and procedures.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Conducted* corroborative inquiry with the IT Audit Specialist and the Manager of Enrollment and Eligibility regarding segregation of duties between individuals performing data entry and the approval and review processes.	No relevant exceptions noted.
	• *Obtained* and *inspected* system generated listing of users within the system including evidence of role based security.	No relevant exceptions noted.
12.3 Through a multi-tiered system, including design, logical and physical security, and segregation restricts data input functions to only authorized personnel. Configuration of security for online work queue systems limit access to only authorized personnel. Access for the system is controlled through three levels: • Application privilege is granted by role. • Database access is controlled by DBA assignment (locked or open). • The operating system administrator will require a user profile for identification setup.	• *Observed* the access rights information for evidence of proper access roles assigned within the system for Data Entry, Eligibility, and Case Corrections.	No relevant exceptions noted.
	• *Inquired* of Technical Infrastructure Manager regarding the control of access in the system. The inquiry response confirmed that access is controlled through three levels: (1) application privilege is granted by role, (2) database access is controlled by DBA assignment (locked or open), and (3) the operating system administrator will require a user profile for identification setup.	No relevant exceptions noted.
	• *Obtained* and *inspected* system generated listing of users within the system that provides evidence of role based security.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
12.4 A hand count of mail items is performed by Mail Operations Specialists when mail is opened. This count is entered into the automated scanner prior to the scan to verify all pieces of information enter the system.	• *Obtained* and *inspected* the documented procedures relevant to the count comparison within the Mail Room. The documentation included: ▪ WI-01-03-02 – Prepare Documents for Scanning, Noted page 3 under section B discusses procedures for hand counting mail items, and ▪ WI-01-03-03 - Document Imaging, page 7 under 8a) explaining check for page count discrepancies.	No relevant exceptions noted.
	• *Tested* the mail count comparison by entering an incorrect count number in the scanner prior to the scan.	No relevant exceptions noted.
12.5 Configuration of online work queue systems route prioritized data and jobs to appropriate personnel.	• *Obtained* and *inspected* documentation for evidence of automated work queues, appropriate triggers and routing. The documentation included following: ▪ PP-03-04 Image Assembly, noting page 3 showing the Image Assembly workflow into all work queues, and ▪ WI-03-04-01 Processing and Linking Document.	No relevant exceptions noted.
	• *Tested* a sample of three (3) different types of mail by tracing from the scanner to the appropriate work queue using the Document Control Number (DCN) to ensure the system is configured to route work appropriately.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
12.6 Data flow within the system is monitored through the use of system reports and metrics to assure timeliness of completion.	• *Obtained* and *inspected* the reports documenting the workflow through the work queues for timeliness. • *Obtained* and *inspected* documentation for the existence of performance measures and the communication of those measures to staff. The following documentation was inspected: ▪ Weekly Tactical Meeting minutes, and ▪ California Healthy Families Program (CAHFP) Performance Standards spreadsheet. • *Inquired* of the Director of Quality Assurance regarding the weekly staff meetings where an agenda item is included for the review of the key metrics.	No relevant exceptions noted. No relevant exceptions noted. No relevant exception noted.
12.7 The system utilizes graphical user interfaces (GUI), predefined forms, and embedded interactive feedback and validation and edit checks to assure efficient and effective processing.	• *Observed* several system screens utilized by the Data Entry, Eligibility, and Case Corrections departments.	No relevant exceptions noted.
12.8 Originating data and source documentation is stored in secure location. The Folsom facility's second floor serves as a storage area for hard documents. They are cataloged and stored by DCN.	• *Inspected* the retention and storage provisions in the contract with the MRMIB including the twelve (12) month retention requirement. In addition, also inspected the, Letter of Instruction 07-10 – Records Retention, which altered the retention period from one year to three (3) months. • *Inquired* of the Mail Operations Manager regarding the storage and retention policy. • *Observed* the process to assure a sample of records were destroyed or retained per contract guidelines.	No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted.

<table>
<tr><th>Controls Specified by MAXIMUS</th><th>Testing Performed by the Service Auditor</th><th>Results of Test</th></tr>
<tr><td>12.9 A log of all requests and movement of hard copies to counties is maintained within the system.</td><td>• <i>Obtained</i> and <i>inspected</i> a sample of reconciliation reports for both AIM and HFP from March 1, 2009 to February 28, 2010, showing all documents that have been sent to requesting counties by county and date.</td><td>No relevant exceptions noted.</td></tr>
<tr><td colspan="3">Control Objective 13: Processing controls provide reasonable assurance that:
• Data is posted to the correct files, completely and accurately.
• Unauthorized changes to data are prevented.
• Database files remain complete and accurate until changes occur as a result of authorized processing.
• Procedures assure that balancing of data is made with relevant control totals. Transaction processing can be traced effectively to reconcile disrupted data.
• Continued integrity of stored data.
• Procedures establish development standards, as appropriate, for electronic transaction integrity and authenticity (atomicity, consistency, isolation, and durability).</td></tr>
<tr><td>13.1 Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive appropriate procedure training for their job responsibilities.</td><td>• <i>Obtained</i> and <i>inspected</i> documentation for inclusion of formalized business related functions. The documentation inspected included:
▪ PP-03-01 – SPE Data Entry,
▪ PP-05-02 – Case Correction Request,
▪ WI-02-02-02 – Initial Receipt and Determination, and
▪ WI-02-02-01 – Missing Info for HFP Apps.</td><td>No relevant exceptions noted.</td></tr>
</table>

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Conducted* corroborative inquires with the Mail Room Manager and Manager of Enrollment and Eligibility regarding the use of documented procedures and work instructions and the training procedures related to input controls.	No relevant exceptions noted.
	• *Obtained* and *inspected* the training curriculum for new hires and continuing education for the inclusion of job specific training.	No relevant exceptions noted.
	• *Tested* a sample of 29 of 688 employees for proper testing by tracing them to passing exam scores for training classes that culminated with an assessment or test where a test is required by the Project.	No relevant exceptions noted.
13.2 Personnel are organized by function and provided access to information systems in terms of job responsibilities. Critical input functions are separate from critical processing functions. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Obtained* and *inspected* documentation for evidence of authority levels and separation of critical functions. The following documentation was inspected: ▪ PP-03-01 – SPE Data Entry, ▪ PP-05-02 – Case Correction Request, ▪ WI-02-02-02 – Initial Receipt and Determination, and ▪ WI-02-02-01 – Missing Info for HFP Apps.	No relevant exceptions noted.
	• *Observed* the data entry and review process for all levels according to the workflow in document PP-03-01 – SPE Data Entry.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Conducted* corroborative inquiries with the IT Audit Specialist and the Manager of Enrollment and Eligibility regarding segregation of duties between individuals performing data entry and performing approval and review processes.	No relevant exceptions noted.
	• *Obtained* and *inspected* system generated listing of users within the system for evidence of role based security.	No relevant exceptions noted.
13.3 Functional quality control (QC) processes are in place and documented. Internal QC is performed by each unit. External QC is performed by Quality Assurance Department.	• *Obtained* and *inspected* documentation for evidence of the existence of the QC function performed in each unit. The following documentation was inspected: ▪ PP-03-01 – SPE Data Entry, ▪ PP-05-02 – Case Correction Request, ▪ WI-02-02-02 – Initial Receipt and Determination, ▪ WI-02-02-01 – Missing Info for HFP Apps, ▪ DE CWD QC Spreadsheets, ▪ Data Entry QA Worksheets, and ▪ Applications Data Entry Specialists activity logs.	No relevant exceptions noted.
	• *Inquired* of the Data Entry Supervisor regarding the process of internal (departmental) and external (Quality Assurance Department) quality control.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Tested* a sample of 27 from a population of 240 SPE entries by tracing them through the data entry process to the final eligibility determination for the performance of a proper review. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2%. ▪ A sampling error rate of 5%.	No relevant exceptions noted.
13.4 Processing reviews 100% of denials, CWD applications and new applications.	• *Obtained* and *inspected* documentation for evidence of the CWD review process. The following documents were inspected: ▪ PP-03-01 – SPE Data Entry, ▪ PP-05-02 – Case Correction Request, ▪ WI-02-02-02 – Initial Receipt and Determination, ▪ WI-02-02-01 – Missing Info for HFP Apps, DE CWD QC Spreadsheets, ▪ Data Entry QA Worksheets, and ▪ Applications Data Entry Specialists activity logs.	No relevant exceptions noted.
	• *Inquired* of the IT Audit Specialist regarding the process of reviewing all denials, CWD applications and new applications.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
	• *Tested* a sample of 27 from a population of 240 SPE entries by tracing them through the data entry process to the final eligibility determination for a proper review process. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2%. ▪ A sampling error rate of 5%.	No relevant exceptions noted.
13.5 The system software design provides field defaults, field locking and field choices which provide database normalization and control data integrity. This is achieved through the system: • FMN assignment • Internal Calculations • Case ID assignment • Address update • Triggers • Form design • Verification • Work queues	• *Observed* the application entry, eligibility, and case corrections screens for the use of the listed control items.	No relevant exceptions noted.
13.6 Batch control and notification is used for the nightly (daily) batch update and posting of transaction records.	• *Conducted* corroborative inquiries of the Director of Systems Administration and the Technical Infrastructure Manager regarding the process of utilizing batch control for the updating and posting of transaction records. • *Tested* the batch updates for deposits by tracing amounts received to the daily batch postings in the subsidiary ledgers.	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
13.7 Necessary case corrections controls exist via special system user interfaces to perform case corrections in special cases. Specially assigned trained users possess special roles with higher privilege (super user) for accessing cases using separate data entry forms available to correct the cases. These users are separate from data entry or eligibility staff. All instances of access to cases within the system is logged automatically and recorded.	• *Obtained* and *inspected* documentation for evidence that there are independent controls around case corrections and case clean up. The following documentation was inspected: ▪ PP-17-23 – Change Action Request CAR, ▪ PP-12-17 – EOM Disenrollment Quality Analysis Plan, ▪ PP-05-02 – Case Correction Request ▪ WI-05-02-04 – Reinstate with Capped Enrollment, ▪ WI-05-02-01 – Generating a Financial Request, ▪ WI-05-02-02 – Add A Person- No Effective Date, and ▪ WI-05-02-03 – AER only give one month due to CE.	No relevant exceptions noted.
	• *Tested* a sample of 30 case corrections from a population of 13822 for evidence that the case correction and/or case decision was made according to documented guidelines. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2%. ▪ A sampling error rate of 5%.	No relevant exceptions noted.
	• *Inquired* of appropriate personnel regarding processing case corrections, and case clean up for evidence that only authorized personnel have ability to perform these duties.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
13.8 A dedicated Research and Appeals unit is responsible for customer interface regarding all disputes.	• *Obtained* and *inspected* documentation for evidence of the definition and responsibilities of the appeals and research area. The following documentation was inspected: ▪ PP-05-01 – HFP Appeals, ▪ WI-05-01-01 – Appeals Process, ▪ WI-05-01-04 – Billing Disputes, ▪ WI-05-01-05 – Creating Case Chronologies, and ▪ Business Rules - Section 18 Appeals.	No relevant exceptions noted.
	• *Tested* a sample of 28 from a population of 409 Appeals by tracing them through the system for evidence that the correct processing and determination occurred. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2% (appropriate sample size). ▪ A sampling error rate of 5%.	One (1) exception out of twenty-eight (28) appeals (0.35%) was noted where the written response was sent on the sixteenth (16th) business day. A response to Appeals that does not require MRMIB review should be made within fifteen (15) business days of receipt. MAXIMUS Response: The appeal was processed within fifteen (15) business days of receipt and upheld. The eligibility re-determination of the case was completed on the sixteenth (16th) business day and resulted in HFP enrollment. Subsequently, the welcome letter to the applicant was generated on the actual completion date of the eligibility re-determination. Problem Statement #66359 has been created for corrective action plans to include a review of relevant Work Instructions for clarity and completeness of procedural descriptions.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
13.9 Daily back-ups are performed and regularly tested. Any errors produced from the backup log are investigated and resolved. Rotation methods are documented and practiced and a log is maintained. Storage of media is securely transported and maintained by Iron Mountain.	• *Obtained* and *inspected* various related documentation including but not limited to: ▪ The backup procedures followed for each system. ▪ The backup logs noting any errors or warnings.	No relevant exceptions noted.
	• *Observed* a successful test restore that was performed and recorded.	No relevant exceptions noted.
	• *Inspected* the inventory of tapes stored at the off-site storage facility.	No relevant exceptions noted.
	• *Inspected* a sample of the log of items stored at the facility noting that the items were present at the facility.	No relevant exceptions noted.
	• *Inquired* of IT support personnel to determine backup procedures.	No relevant exceptions noted.
	• *Inspected* backup logs evidencing successful backups.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 14: Output controls provide reasonable assurance that: • Procedures define the handling and retention of output. • Procedures define and assure appropriate processing and distribution of output. • Procedures define and assure appropriate physical and logical access to output. Confidentiality of output is defined and taken into consideration in the procedures. • Procedures assure that both provider and user review output for accuracy and that procedures control errors contained in output. • Physical access to output printers and subsequent storage areas is restricted to authorized personnel.		
14.1 Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive appropriate procedure training for their job responsibilities.	• *Obtained* and *inspected* documentation for evidence of business related functional process flows. The documentation inspected included: ▪ PP-03-01 – SPE Data Entry, ▪ PP-05-02 – Case Correction Request, ▪ WI-02-02-02 – Initial Receipt and Determination, and ▪ WI-02-02-01 – Missing Info for HFP Apps. • *Tested* a sample of 29 of 688 employees by inspecting the employees training records for completeness and timeliness.	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
14.2 Personnel are organized by function and provided access to information systems in terms of job responsibilities. Critical input functions are separate from critical processing functions. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Obtained* and *inspected* documentation for evidence of the approval and review process with corresponding authority levels. The inspected documentation included: ▪ PP-03-01 – SPE Data Entry, ▪ PP-05-02 – Case Correction Request, ▪ WI-02-02-02 – Initial Receipt and Determination, WI-02-02-01 – Missing Info for HFP Apps,	No relevant exceptions noted.
	• *Observed* data entry and review processes within all authority levels according to the workflow in SPE Data Entry.	No relevant exceptions noted.
	• *Observed* all authority levels within the AIM data entry and review process according to the workflow in SPE Data Entry.	No relevant exceptions noted.
14.3 System software design provides field defaults, field locking and field choices which control data integrity for data output. This is achieved through the system: • Triggers • Letter file generation • Filtered date-driven restrictions • 2D Barcode (KP Corp)	• *Observed* data entry and eligibility process screens for evidence of the automatic use of field defaults, field locking and field choices to control data integrity.	No relevant exceptions noted.
	• *Inspected* the system application for the use of triggers, letter file generation, date driven restrictions and barcodes.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
14.4 Batch control exists within the system using a dedicated IT technician with 24X7 online monitoring for batch jobs. The batch control is used for the following: • Outbound letter files • Mail count comparisons • Reporting of PDF images (counts) • Capitation calculation and preparation of 820 and 834 files.	• *Inspected* documentation for the existence and usage of batch controls. The documentation inspected included: ▪ Capitation Processing, ▪ Mail Operations – Outgoing, ▪ Mail Operations – Incoming, ▪ Printing for the Daily Letter Production, ▪ Inserting Daily Letter Production with Bell & Howell Inserter, and ▪ CWD Pulls.	No relevant exceptions noted.
	• *Observed* the procedure for mail count comparisons for evidence that standard procedures exist and are being used.	No relevant exceptions noted.
	• *Inspected* letter formats within QMS, verifying correct use of the format in a sample of outbound client correspondence. (Note the same sample was used in 14.5)	No relevant exceptions noted.
14.5 Outbound correspondence makes use of pre-designed forms and letters that have been approved by the MRMIB and are stored in QMS.	• *Inspected* documentation for the existence and use of the pre-designed forms. The documentation inspected included: ▪ Mail Ops Outgoing, ▪ Printing for the Daily Letter Production, and ▪ Daily Letter Production Report.	No relevant exceptions noted.
	• *Inspected* selected letter formats within QMS, verifying the correct use of the format in a sample of outbound client correspondence.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
14.6 Error handling procedures are in place for the handling of: • Returned mail • Letter exceptions • 834 and capitation file exceptions	• *Obtained* and *inspected* documentation for the existence of error handling procedures. The documentation inspected included: ▪ 834 Exception Processing, ▪ Monitoring and Control of Nonconforming Product in Information Systems, and ▪ Prepare Documents for Scanning.	No relevant exceptions noted.
	• *Observed* the returned mail process for evidence that mail is bound into groups and hand counted.	No relevant exceptions noted.
14.7 Activity reporting and monitoring includes a set of predefined procedures for developing reports and routine report generation for monitoring output and performance.	• *Obtained* and *inspected* documentation for the existence of activity reporting. The documentation inspected included: ▪ Report Development, ▪ EOM Reporting Plan, ▪ Daily Letter Production Report, and ▪ Ad Hoc Request.	No relevant exceptions noted.
	• *Inquired* of the Director of Human Capital regarding the procedures for activity reporting and monitoring.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
14.8 AIM and HFP provider plan capitation (Health, Vision, and Dental) is computed correctly using rate tables provided by the MRMIB. The amounts reported to the MRMIB are correctly allocated and summarized based upon the abortion supplement (allowable funding) and the participant's legal immigration status.	• *Inspected* the 820 files for the period from March 1, 2009 to February 28, 2010.	No relevant exceptions noted.
	• *Inspected* the county number table.	No relevant exceptions noted.
	• *Inspected* the capitation rates tables from MRMIB, provided to the Project, used to compute the capitation amounts.	No relevant exceptions noted.
	• *Tested* capitation processing by re-computing capitation for the provider plans independently from the system using generalized audit software tools.	No relevant exceptions noted.
	• *Verified* the capitation amounts computed independently to those computed by the system and reported in the AIM and HFP 820 files for the period.	Noted one (1) exception with six (6) instances of the five million one hundred eighty four thousand and eight hundred and fourteen (5,184,814) records, where HFP Health Plan capitation was overpaid. MAXIMUS Response: The error rate for this exception, caused by using an incorrect capitation rate, is less than 0.0001157% (6 instances/5,184,814 records audited). Per Policy Letter 07-02, MRMIB directed MAXIMUS to avoid dual coverage for AIM-linked babies. Due to a low number of retro-enrollments for AIM babies and the eligibility gaps and plan coverage differences between the HFP and Medi-Cal programs, the HFP capitation for retro-enrollment of AIM-linked babies is inserted manually.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
		The identified capitation discrepancies were a result of incorrect manual allocation of capitation related to the consolidation and insertion of AIM Baby lump sums. This issue was previously identified as a result of the October 2009 Internal Audit of Capitation which covered the audit period of March 1, 2009 to August 31, 2009, overlapping with this audit's period of March 1, 2009 to February 28, 2010. Problem Statement #62462 was closed on June 15, 2010, after the implementation of the Corrective Action Plan, which included recoupment and repayment of correct amounts.
14.9 An Independent Rate Verification is performed to assure the use of appropriate rates in the capitation calculation.	• *Obtained* the applicable provider rate tables for the grant years being tested from the MRMIB (independent verification of the rates).	No relevant exceptions noted.
	• *Compared* the HFP provider rates obtained independently from the MRMIB to those used for computation of capitation in the system.	No relevant exceptions noted.
	• *Compared* the Access for Infants and Mothers (AIM) provider rates obtained independently from the MRMIB to those used for computation of capitation in the system.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
14.10 Allowable Funding for the Program is tracked and reported to MRMIB on a monthly basis including the abortion rate supplement.	• *Obtained* the "Funding Split" reports for each month for the period March 1, 2009 to February 28, 2010.	No relevant exceptions noted.
	• *Selected* a sample of 53 month-plan combinations from a population of 198 month-plan combinations derived from the 820 files (Payment Order and Credit Advice) from March 1, 2009 to February 28, 2010. Parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2%. ▪ A sampling error rate of 5%.	No relevant exceptions noted.
	• *Tested* the capitation computation by comparing the independently computed totals to the amount presented for abortion rate supplement on the "Funding Split" report.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
14.11 Eligibility verification includes: • Capitated participants are eligible for participation in the program. • Information provided in the 820 capitation files corresponds to the information contained in the case management system. • Where recoupments have been performed they were needed and correctly computed and performed. • The amounts reported to the MRMIB are correctly allocated and summarized based upon the abortion supplement (allowable funding) and the participant's legal immigration status.	• *Tested* eligibility by selecting a sample of 30 from a population 431,369 from the 820 files (Payment Order and Credit Advice) for the period March 1, 2009 to February 28, 2010. The parameters for the sample were: ▪ A 95% Confidence level. ▪ An expected error rate in the population of 2%. ▪ A sampling error rate of 5% Tested the detailed participant information to the enrollment form image retained in the system. Attributes tested included: ▪ Age on application agrees to 820 age category code; ▪ Income and family size on the application qualify client for HFP and/or AIM; ▪ Plans selected per application or other documentation agree to the appropriate 820 capitation files; and ▪ Citizenship or immigration documentation is appropriately stored in the case file. ▪ Manually calculated eligibility based on the information contained on the application form.	No relevant exceptions noted.
	• *Tested* for proper disenrollment processing by using the above enrollment sample of and traced them to the system to ensure the disenrollments were performed appropriately.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Systems Application Processing Controls – Financial Management Systems		
Control Objective 15: Input controls provide reasonable assurance that: • Originating HFP and AIM source data enters into Oracle Financials through trained and authorized persons, data preparation procedures are established and followed to minimize errors and omissions and to allow the input of only valid data into the system. • Automation is used where possible to reduce errors, increase efficiency and route priority work. • Authorized source documentation and data is complete and accurate, properly accounted for, and transmitted in a timely manner. • Error handling procedures detect errors and irregularities and report them for corrective action. • Source documents are retained and available for reconstruction and legal compliance.		
15.1 Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive appropriate procedure training for their job responsibilities.	• *Inspected* documentation evidence of business related functional process flows. The documentation inspected included: ▪ Accounts Payable Reconciliation with GL documentation, ▪ Accounts Receivable Reconciliation with the GL documentation, and ▪ Applicable Business Rules.	No relevant exceptions noted.
	• *Inquired* of Training Management as to the training employees must complete for their position.	No relevant exceptions noted.
	• *Tested* a sample of 29 of 688 employees to their respective training records for completeness.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
15.2 Personnel are organized by function and provided access to information systems in terms of job needs. Critical input functions are separate from critical processing functions. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Conducted* corroborative inquiries of the Director of Accounting and the Director of Compliance regarding segregation of duties in the finance department. • *Inspected* organizational charts and job descriptions for finance personnel for evidence of segregation of functional activities and personnel.	No relevant exceptions noted. No relevant exceptions noted.
15.3 Access and security includes the granting of access rights to the financial application based upon job responsibilities and approval by the application owners via a multi-tiered system design.	• *Obtained* and *inspected* the access lists for Oracle Financials for evidence of appropriate access rights. • *Inquired* of the director of accounting (the Oracle Financials application owner). The Oracle Financials application access must be authorized by the Director of Finance.	No relevant exceptions noted. No relevant exceptions noted.
15.4 Automated input systems are utilized where possible.	• O*bserved* data entry functions with regard to automated input systems. • *Inquired* of appropriate management personnel noting that transactions failing edit and validation routines are posted to a suspense file.	No relevant exceptions noted. No relevant exceptions noted.
15.5 Documented procedures for the correction of errors and out-of-balance conditions and entry of overrides exist and are effectively communicated to appropriate personnel.	• *Obtained* and *inspected* documentation for evidence of error correction procedures. The documentation inspected included: ▪ Processing Premium Adjustments, ▪ Accounts Payable Reconciliation with GL, and ▪ Accounts Receivable Reconciliation with the GL.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
15.6 Configuration of online work queue systems route prioritized data and jobs to appropriate personnel.	• *Obtained* and *inspected* documentation for evidence of the work queue routing system used for prioritizing data and jobs. The documentation inspected included: ▪ AIM Processing documentation, ▪ HFP Processing documentation, ▪ DE CWD QC Process documentation, ▪ Oracle Financials Systems EFT Process documentation, and ▪ 834 File Processing documentation.	No relevant exceptions noted.
15.7 Data flow is monitored through manual and application processes.	• *Inquired* of the Project's Director of Accounting as to the procedures in place for online data monitoring.	No relevant exceptions noted.
	• *Obtained* and *inspected* a copy of the non-conformance log for completeness noting conformity with stated policy.	No relevant exceptions noted.
15.8 To assure data accuracy, completeness and the ability to assure authenticity checks, transactions are input as close to the point of origination as possible. In addition, the close proximity to the data origin affords less effort in both validation and correction of data entry when necessary.	• *Inspected* process maps and noted that with the exception of manual adjustments all data enters Oracle Financials via batch process from outside sources: ▪ Cash Receipts – Lockbox and EFT. ▪ Invoicing – Updated from the system. ▪ Refunds – Updated from the system.	No relevant exceptions noted.
	• *Inquired* of the Project's Director of Accounting that these are all close to the source origin of the transaction.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
15.9 Originating data and source documentation are stored for retention needs. The Folsom facility's second floor serves as a storage area for hard documents, and electronic data is stored at Iron Mountain.	• *Inspected* the storage and retention policy. • *Inquired* of the Central Operations Director as to the storage and retention policies and procedures. • *Observed* the storage facility and viewed filing process.	No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted.
Control Objective 16: Processing controls provide reasonable assurance that: • Data is posted to the correct files, completely and accurately. • Unauthorized changes to data are prevented. • Database files remain unchanged until authorized processing occurs. • Procedures assure that balancing of data is made with relevant control totals. Transaction processing can be traced effectively to reconcile disrupted data. • There is continuity and integrity of stored data. • Procedures establish development standards, as appropriate, for electronic transaction integrity and authenticity (atomicity, consistency, isolation, and durability).		
16.1 Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive appropriate procedure training for their job responsibilities.	• *Inspected* Oracle Financials Systems EFT Process documentation for completeness. • *Inquired* of Training Management as to the training employees must complete with respect to their position. • *Tested* a sample of 29 of 688 employees to their respective training records for completeness.	No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
16.2 Personnel are organized by function and provided access to information systems in terms of job needs. Critical input functions are separate from critical processing functions. Approval and review processes are constructed to match authority levels, provide cross-functional oversight, and ensure contractual performance.	• *Conducted* corroborative inquiries with the Project's Director of Accounting and the Director of Compliance as to the procedures in place. • *Observed* controls in place with regards to segregation of functional activities and personnel.	No relevant exceptions noted. No relevant exceptions noted.
16.3 Processing reviews 100% of NSF, ACH returns and Refunds	• *Inspected* documentation for evidence of formalized work instructions for the processing review functions. The documentation inspected included: ▪ Reversal of Returned items, ▪ NSF Check Reversal, and ▪ Refund Invoice Inquiry. • *Inquired* of the Project's Director of Accounting as to the procedures in place regarding processing reviews of NSF and ACH returns and refunds.	No relevant exceptions noted. No relevant exceptions noted.
16.4 Standard Oracle Financials Forms (input screens) are used for interactive data entry into the financial system. Wherever possible, field verification and limits checking is performed.	• *Inquired* of the Project's Director of Accounting as to the Financial Forms used with regards to field verification and limits checking controls in the software design. • *Observed and inspected* various screens for evidence of field verification and limits checking.	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
16.5 Batch Control exists within the Oracle Financials and all interfaces with applications and data outside Oracle Financials. Batch errors are logged and logs are inspected.	• *Inquired* of the Project's Director of Accounting as to procedures in place to obtain Batch Control.	No relevant exceptions noted.
	• *Obtained* and *Inspected* a sample of dates for cash receipts from: ▪ Aquracy – HFP (62) AIM (61) ▪ Credit Card 36 ▪ EFT (all months) ▪ Western Union 61	No relevant exceptions noted.
	• *Tested* batches to assure that the batch total transferred agreed to the file total, then traced to the posting in Oracle Financials (for both HFP and AIM).	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
16.6 Reconciliations are performed as follows: • Bank records are reconciled on a daily basis to appropriate Sub-Ledger activity. • General Ledger Cash accounts are reconciled on a monthly basis to bank records. • General Ledger Accounts Receivable and related accounts are reconciled on monthly bases to detailed records • General Ledger Accounts Payable and related accounts are reconciled on monthly bases to detailed records. • General Ledger control accounts are reconciled on a monthly basis to subsidiary ledger accounts on a current and regular basis. • Reconciliations are Inspected and approved on a regular basis.	• *Inspected* documentation for evidence of the reconciliation process. The documentation inspected included: ▪ Reconciliation of the MRMIB collection, ▪ Reconciliation for Refunds, ▪ Accounts Payable Reconciliation with the General Ledger, and ▪ Accounts Receivable Reconciliation with the General Ledger.	No relevant exceptions noted.
	• *Inquired* of various finance staff to confirm the use of the QMS procedures and the use of the reconciliation process.	No relevant exceptions noted.
	• *Tested* a sample of the Detailed Ledger records by tracing entries to the General Ledger postings.	No relevant exceptions noted.
	• *Tested* a sample of the accounts receivable reconciliations and accounts payable reconciliation by tracing source information (subsidiary records) to the reconciliation and agreeing the balance amounts to the general ledger control accounts.	No relevant exceptions noted.
	• *Tested* a sample of 30 from a population of 2,271 AIM refunds processed and 30 from a population of 40,410 HFP refunds processed to their respective reconciliation and agreed the amounts to that actually disbursed per the image records.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
16.7 Daily backups are performed and regularly tested. Rotation methods are documented and practiced and a log is maintained. Storage of media is maintained at Iron Mountain location.	• *Inspected* documentation for evidence of the backup procedure and tape rotation process. The documentation inspected included: ▪ the backup procedures followed for each system, and ▪ the backup logs noting any errors or warnings.	No relevant exceptions noted.
	• *Inspected* the log of items stored at the off-site storage facility	No relevant exceptions noted.
	• *Inspected* a sample of the log of tapes stored at the facility with the tapes present at the facility.	No relevant exceptions noted.
	• *Inquired* of IT support personnel to determine backup procedures.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
Control Objective 17: Output controls provide reasonable assurance that: • Procedures define handling and retention of output. When negotiable instruments are produced, special care should be taken to prevent misuse. • Procedures define and assure appropriate distribution of IT output. • Procedures are communicated for physical and logical access to output. Confidentiality of output is defined and taken into consideration in the procedures. • Procedures assure that both provider and user review output for accuracy and that procedures control errors contained in output. • Physical access to output printers and subsequent storage areas is restricted to authorized personnel.		
17.1 Written procedures and work instructions establish business-related functional process flows and define job tasks. Personnel receive appropriate procedure training for their job responsibilities.	• *Obtained* and *inspected* the Oracle Financials Systems EFT Process document for evidence of formally documented functions. • *Inquired* of Training Management as to the various training employees must complete. • *Tested* a sample of 29 of 688 employees to documentation showing that they have completed necessary training for their respective positions.	No relevant exceptions noted. No relevant exceptions noted. No relevant exceptions noted.
17.2 Oracle Financial Software is designed with triggers and reporting.	• *Inquired* of the Project's Director of Accounting as to the various triggers and reporting of the Oracle Financial Software Design. • *Observed* that the Oracle Financial Software is designed with triggers and reporting.	No relevant exceptions noted. No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
17.3 Refund Output Controls include: • Refund processing produces an output file (the initial run) to be used by the State of California for approval prior to the final disbursement of refund checks. Once approved, a final run is produced and an outsourced vendor file for disbursement processing is created. • The sequential numbering profile option for the disbursements has been enabled and is in use to control the check numbers produced by the outsource vendor. • Hash totals are used for the payment, address and client information. The Hash totals are produced during the initial run and compared to the final run. Any changes will cause the processing of the outsource vendor file to abort and the error is written to a log for further review.	• *Inspected* various QMS documentation including: ▪ Refunds (Overpayments) ▪ Reconciliations (Refunds, Voids) ▪ Returned (Un-cashed Refund) ▪ Reversing a Refund ▪ Refund Invoices Inquiry ▪ Manually Paying Refunds ▪ Manually Voiding Refunds	No relevant exceptions noted.
	• *Obtained* and *tested* a sample set of refunds batched from the period verifying that they were processed according to the stated procedures.	No relevant exceptions noted.
	• *Inquired* of appropriate personnel as to policies and procedures set in place for Refund Output Controls.	No relevant exceptions noted.
17.4 The Oracle Financials “Auto Invoice Process” will not run against all of the records in the open interface table creating customer invoices until a series of validations are completed.	*Inquired* of the Project’s Director of Accounting as to the process of invoicing output controls.	No relevant exceptions noted.

Controls Specified by MAXIMUS	Testing Performed by the Service Auditor	Results of Test
17.5 Error handling procedures for output are documented and followed.	• *Inspected* documentation for the existence of formal error handling procedures. The documentation inspected included: ▪ Void Process for Returned Refund Checks, and ▪ Systems – Monitoring and Controls of Nonconforming Product.	No relevant exceptions noted.
	• *Inquired* of the Project's Director of Accounting and noted that carve-out files are produced with the errors and are inspected.	No relevant exceptions noted.
17.6 Activity Reporting / Monitoring includes: • Procedures for developing reports exist. • Routine reports are generated for monitoring output and performance.	• *Inquired* of the Project's Director of Accounting regarding the procedures for developing reports as well as the frequency and generation of routine reports for monitoring the output and performance.	No relevant exceptions noted.
	• *Inspected* routine reports produced by the system noting conformity with stated policy.	No relevant exceptions noted.